***Why are standards important for IT security and privacy?***

Standards are essential for human civilization. Standards enable the global interoperability of technical solutions while ensuring that the technical progress can be applied smoothly on a global scale. Without international standards it would be much more difficult to interact with partners in different countries or on different continents. This proved to be important for the first time during the industrial revolution more than 100 years ago, and became even more important as globalization progressed. In the past, we have seen that any technology of importance has been accompanied by mechanisms to ensure its safety and security, and that the availability of such mechanisms was an indication for the maturity of these technologies. These former technologies included the steam engine and the automobile, to mention but a few. Today, information and communication technology is one of the key technologies and may very well be the most important one of our time.

In terms of function, computer networks have now reached tremendous performance levels, computers are everywhere, and artificial intelligence is leveraging the algorithmic capabilities of IT systems to unprecedented levels. Some people say that these developments are at least as important as the industrial revolution a century ago. Similar to the mechanisms that ensured the safety of steam engines in the past, society today needs mechanisms to protect us from the risks we face due to IT systems. And this is where IT security and privacy standards come into play. Since the very Web itself is global, IT security and privacy need to be considered on a global level too. International standards have proven to be a good tool when it comes to reaching a global scale.

Neither IT security nor privacy can be addressed in a simple manner. There is no such thing as: "The IT security". There are many approaches to a vast range of challenges. But they can all be categorized and their impact can be measured and evaluated with respect to common rules developed by an

international community of experts. Requirements and recommendations like these determine the value of international standards because they were developed by applying best practices and the wisdom of a countless number of experts from many different countries. In this sense, standards educate the industry, they help avoid unnecessary mistakes, and they support the efficient use of intellectual resources.

The aspect of privacy is even more complicated. While IT security aspects are evaluated more or less similarly around the globe, privacy issues are influenced by cultural and societal factors. It is a matter of fact that different countries or regions have different cultural backgrounds, different traditions, and different legislation on data protection and privacy. This makes it all the more important to define a common vocabulary on privacy concepts, and to make the privacy features and properties of IT systems or applications measurable and comparable. The best way to achieve this is to develop sound and appropriate international standards.

IT security has departed from its niche as a topic of interest merely for governments, the military and the financial sector and has become relevant to everyone who owns a computer or smartphone, i.e. virtually to all of us. Coming full circle with the industrial revolution: IT technology will reach maturity and will be trusted by society as soon as we have a set of well-established international standards in place that covers all relevant aspects of IT security and privacy.

***What is ISO/IEC JTC1's role in IT security and privacy standards? What part is SC 27 playing?***

In global terms, JTC 1, the parent committee of SC 27, is, as its name "Information Technology" suggests, the leading committee on IT standardization. Within JTC 1, SC 27 is responsible for developing standards on information security management, IT security, cryptography, security management, IT security evaluation, data protection, privacy and other related topics. Past experience has shown that security and privacy related topics like these have become more and more cross-sectional and interdisciplinary. This means that topics covered by SC 27 become more relevant for many application areas, not just for information technology. This importance is indicated by the more than 70 committees and organizations liaising with SC 27, proving that there is a need to support many standardization domains with IT security and privacy standards. Almost half of these liaisons connect SC 27 with other JTC 1 committees.

Admittedly SC 27 does attract a large number of highly renowned experts in their respective fields who have been delegated to SC 27 by its current 52 Participating and 25 Observing Members but maintaining these liaisons would consume a lot of resources. JTC 1 serves as a platform that enables easier exchange with its other committees and bundles the forces of its committees in order to develop standards much faster, easier and with optimal quality. What's more, SC 27 is in the comfortable position that many of our expert delegates work in several standardization committees, complementing the official liaison efforts in a very target-oriented manner.

But our liaisons are not one-way streets. SC 27 too supports other committees, providing them with the expertise of SC 27 and regularly making use of their domain knowledge in our standards.

SC 27 has meanwhile published 178 International Standards, and is currently running projects to develop 64 new standards. This perfectly illustrates the high and even growing importance of SC27 in standardization business. As we all know, standards are developed by contributions that come from individual experts who dedicate time and effort to the topics they are heavily involved with. The

large and growing number of published standards indicates that SC 27 is continuously attracting contributing experts who are delegated by many National Bodies and who represent more or less the entire IT industry - once again demonstrating the enormous importance of the activities by SC 27.

***What lies ahead for SC 27 in the years to come?***

If we take a closer look at SC 27 and its history, we can see how SC 27 evolved over the past 25 years. It has grown in terms of the experts participating in its standardization projects, in terms of the Participating and Observing Members, the projects under preparation, and in terms of the different topics addressed. This development is highlighted by the structure of SC 27which is made up of five working groups:

- WG 1 Information security management systems
- WG 2 Cryptography and security mechanisms
- WG 3 Security evaluation, testing and specification
- WG 4 Security controls and services
- WG 5 Identity management and privacy technologies

These working groups cover several aspects of SC 27's focus areas of work. All of these aspects have ongoing relevance to our work while their impact on technology and society is increasing. SC 27 started out with information security techniques and cryptography, security management systems were included at a later stage; its newest field of work is the thematic complex of identity management and privacy. Many of our projects have to be continuously maintained and extended to new application fields. It would be not fair to mention only a few of these projects; SC 27 is currently working on many important projects. Some of them might be more well-known than others, e. g. the information security management standards covered by ISO/IEC 27000 series and the evaluation criteria for IT security (Common Criteria) in the multipart standard ISO/IEC 15408.

Within SC 27, we maintain cooperation between the working groups through regular exchange between the delegated experts. As all SC 27 working groups meet parallel twice a year, the experts may move between the groups, keeping information flowing. However, we have come to see that the growing number of topics calls for the involvement of experts from several communities and committees. In order to address such close cooperation and to accelerate the joint development of standards, we will need to travel down new roads. One option could be to set up joint working groups between SC 27 and other committees. SC 27 has already initialized such a joint working group with ISO TC 307 "Blockchain and distributed ledger technologies" and we are hopeful that this will be successful. It is quite likely, however, that we will need other mechanisms as well if we are to be able to responsively develop more new standards in line with needs in an even shorter space of time.

SC 27 will face a number of technological challenges in the coming years. Emerging technologies will grow and need to be enhanced with security aspects. These technologies include, for instance, the Internet of Things, Smart Cities, or Distributed Ledger technologies, to name just a few. It is foreseeable that any item that can be distinguished and seen as an individual will soon have to have its own identity. And that identity will need to be a secure identity. There are some expectations that the transition brought about by emerging technologies will be quite disruptive; SC 27’s task is to enable the maintenance of IT security aspects and to support the development of interoperable IT security methods required to serve future needs.

But this is only one aspect. SC 27 and its experts are also aware of their responsibility to develop good standards that allow privacy aspects to be considered in an appropriate manner. In the past, preventing harm meant ensuring that a steam engine did not explode. In today's IT systems, this also means preventing data misuse, especially the misuse of personal data. Even if there is no international consent on the exact content of privacy rules, SC 27 is determined to provide best practice experiences and to develop measures to describe and evaluate different, conceivable levels of privacy protecting technology in order to allow a precise description and a useful comparison of products and systems.

Last, but not least, SC 27 has what could be described as a luxury problem. As the SC 27 community is growing rapidly, and as our meetings attract an ever-increasing number of experts, it is becoming more and more difficult for the National Bodies to host upcoming events. The perfect organization with excellent logistics, which is provided by the meeting hosts and which is highly appreciated by all participants, requires enormous effort, and is in no way trivial. Sometimes, simply finding meeting facilities and hotel rooms to host five working groups and their experts is a challenge, not to mention that almost all of the working groups are additionally split into sub-groups. A perfectly organized event for participants involves an incredible amount of hard work behind the scenes for the host.

Meeting time is limited, and the number of projects is growing. We now need to find new ways to make our work more efficient, e.g. by focusing meetings on the work that needs to be carried out there and preparing as much as possible in advance, or by organizing meetings in a more compact way. This kind of optimized organization is a task for management staff: the chairpersons, the secretariat, and the conveners. Fortunately, they are supported by the Management Advisory Group, a panel of highly renowned SC 27 experts.

***Can you tell us about your experience in developing standards, and why you are interested in IT security and privacy?***

The first time I consciously came across an International Standard in my business life was more than a decade ago when I was responsible for the Common Criteria evaluation of a biometric speaker recognition system from the manufacturer's perspective. As it happened, CC is today an SC 27 standard. This brought me in touch with some standardization groups at DIN, the German Institute for Standardization. The one I decided to become a member of was NIA-37, the mirror of SC 37 "Biometrics". During that time, I started working with one of the major players in the fingerprint industry, and so it was quite a logical decision for me to become involved in biometrics standardization. At the same time, I also developed an affinity to border control technologies which brought me closer to SC 17 "Cards and security devices for personal identification" and SC 31 "Automatic identification and data capture techniques".

Now, working for Bundesdruckerei, the German State Printer, I am the editor of ISO/IEC 19794-5 and ISO/IEC 39794-5, the facial image data format standards which are mostly applied in passports and other Machine Readable Travel Documents (MRTDs). Furthermore, I am the editor of ISO/IEC TR 29196 "Guidance for biometric enrolment" in SC 37. In SC 17, I am the editor of the ICAO Portrait Quality TR and in SC 31 one of the two editors of ISO/IEC 30116 which deals with the machine readability of the Machine Readable Zone of an MRTD. I am the liaison officer between SC 37 and CEN/TC 224 and from SC 37 to SC 17. Additionally, I convene CEN/TC224 Working Group 19 which deals with breeder documents.

All of these topics have certain security aspects which are becoming increasingly important. It was therefore a natural step for me to extend my standardization work to SC 27. I especially saw for myself the close connection between IT security, privacy, and biometrics since I was involved in the development of passport, passport inspection, and border control technology. Several projects, the most important one probably being FIDELITY, funded by the European Commission in the Seventh Framework Programme, led me closer into the interconnection between new ID management technologies, data handling, IT security, and privacy considerations.

Participating in SC 27, I saw that I already knew many of the experts working in this committee from my standardization activities in the past. Taking into account the cross-sectional character of IT security and privacy, this did not come as a surprise. In recent years, and fulfilling several roles in standardization groups, I have learned a lot about the power of qualified consent as the fundamental concept on how to write good standards. It is therefore both a challenge and a pleasure to me to chair SC 27, and to support our experts in their effort to strive for good IT security and privacy standards. The chairmanship is mostly a service role, and sometimes it is a guidance and leadership role. But it is always a task that allows me to work with many good experts from all over the world, where I can learn from them and share my experiences with them. In that sense, I am happy to be elected to serve as the next Chair of SC 27.

***Are there other organizations or committees also working in this area? What are their relationships to SC 27?***

As information security management, IT security and privacy have always been cross-sectional and interdisciplinary issues, it is no wonder that SC 27 has many interfaces with other organizations. Besides traditionally IT-sensitive sectors (banking, government or the military), upcoming application domains (smart home, smart cities or IoT) have now come to understand their need for IT security. This means that the number of partners applying SC 27 standards or referring to SC 27 standards in their own products is growing quickly. Additionally, SC 27 receives more and more requests to develop products for specific application domains.

SC 27 liaises with more than 70 organizations, including JTC 1 sister committees and other groups from other standardization organizations like ISO, IEC, ITU, CEN, CENELEC, or ETSI, to mention but a few. We also liaise with industrial organizations and project consortia. All this illustrates the recognition that SC 27 has in the IT security and privacy community. We always strive to make everyone aware of our standardization topics and to avoid duplicate work. Finally, it does not necessarily matter that much who wrote a certain standard, as long as there are no competing standards and as long as standards are comprehensive, applicable and accepted. Sometimes, it is the best choice to develop standards in SC 27, while at other times, it makes more sense to liaise with a partner and to ensure SC 27's expertise is reflected in the partner's document. Developing standards is not a purely academic exercise; it is performed by stakeholders who have strong interests, both commercial and political. After all, the market needs standards that support stakeholders working on certain problems, and these standards are needed quickly, in high quality, and tailored to the needs of all countries.

All the standardization committees I have worked with in the past have developed a very enjoyable culture of cooperation. Arguments are the major force, and consensus is reached by moderating the interests of all stakeholders. This does not mean that there are no conflicts between the participating experts and National Bodies. But SC 27, like all other standardization committees, and in particular,

all of its experts and officers, is committed to resolving such conflicts, to reaching consensus and to developing standards that are as good as possible. This is one of the sources of joy when working with SC 27.